Ehsanul Kabir

State College, PA

(603) 306-9511
ekabir@psu.edu

Research Interests

My research focuses on understanding the factors underlying privacy and security vulnerabilities in machine learning and designing principled defenses. Specific interests include attribute inference, individual record-level vulnerability estimation, and defenses against poisoning attacks in federated learning.

Education

Pennsylvania State University

Ph.D. Candidate, Computer Science and Engineering *Jan 2023 - Now*

- Thesis: Mitigating Privacy Risks and Enhancing Security in Machine Learning Frameworks
- Advisor: Dr. Shagufta Mehnaz

Pennsylvania State University

M.S., Computer Science and Engineering *Jan 2023 - Dec 2024*

- MS Thesis: Towards Secure Federated Learning: A Validation-Based Approach to Mitigating Poisoning Attacks
- Advisor: Dr. Shagufta Mehnaz

Bangladesh University of Engineering Technology

B.S., Computer Science and Engineering *Jul 2014 – Oct 2018*

- Undergraduate Thesis: Estimating Genetic Risk of Diseases of Populations of Different Regions
- Advisor: Dr. Atif Hasan Rahman

Research and Work Experience

Department of Computer Science and Engineering, Pennsylvania State University

Research Assistant *Jan 2023 - Now*

- Client-level attribute inference in federated learning: vulnerability factors and amplified privacy leakage through poisoning.
- Individual record-level vulnerability estimation and defenses against attribute inference that preserve model utility [USENIX '26].
- Understanding and mitigating disparate vulnerability to attribute inference across demographic groups [USENIX '25].
- Client-side validation for defending federated learning against poisoning attacks [S&P '24].
- Research funded by NSF Grants 2613659 and 2442825.

Department of Computer Science, Dartmouth College

Research Assistant *Sep 2021 – Dec 2022*

- Privacy risks of attribute inference through black-box access to classification models [USENIX '22].
- Sentence reconstruction and disclosure of private text from pre-trained language model embeddings [PETS '23].

Samsung R&D Institute Bangladesh

Software Engineer *Dec 2018 – Oct 2019*

- Developed and maintained device automation and user interface features for the SmartThings iOS app using Swift.

Publications

Peer-Reviewed Publications:

[1] Kabir, E., Sultana, N., Li, N., & Mehnaz, S. Can we estimate the privacy vulnerability of individual records? Towards Mitigating Attribute Inference Attacks on ML Models. In 35th **USENIX Security** Symposium, 2026.

[2] Kabir, E., Craig, L., & Mehnaz, S. Disparate privacy vulnerability: Targeted attribute inference attacks and defenses. In 34th **USENIX Security** Symposium, 2025.

[3] Song, Z., Kabir, E., & Mehnaz, S. GNNBleed: Inference Attacks to Unveil Private Edges in Graphs with Realistic Access to GNN Models. Proceedings on Privacy Enhancing Technologies (**PETS**), 2025.

[4] Kabir, E., Song, Z., Rashid, M. R. U., & Mehnaz, S. FLShield: A validation-based federated learning framework to defend against poisoning attacks. In IEEE Symposium on Security and Privacy (**IEEE S&P**) (pp. 2572-2590), 2024. Presentation video: https://www.youtube.com/watch?v=pCmWKOvjfBc

[5] Gu, K., Kabir, E., Ramsurrun, N., Vosoughi, S., & Mehnaz, S. Towards Sentence Level Inference Attack Against Pre-trained Language Models. Proceedings on Privacy Enhancing Technologies (**PETS**), 2023.

[6] Mehnaz, S., Dibbo, S.V., Kabir, E., Li, N., & Bertino, E. Are your sensitive attributes private? Novel model inversion attribute inference attacks on classification models. In 31st **USENIX Security** Symposium, (pp. 4579-4596), 2022.

In Review:

[1] Song, Z., Kabir, E., Gong, N., & Mehnaz, S. Evolving Embeddings, Emerging Leaks: Inference Attacks on Dynamic GNNs. Under review at 36th USENIX Security Symposium , 2027.

Teaching Experience

Department of Computer Science and Engineering, Pennsylvania State University
Teaching Assistant *Jan 2023 – Now*

- Co-designed a novel machine learning security project for the graduate-level *Introduction to Computer Security* course in collaboration with Dr. Shagufta Mehnaz.
- Delivered guest lectures detailing project specifications and facilitated weekly office hours to support student learning.
- Evaluated and graded complex technical projects for graduate students.

Department of Computer Science, Dartmouth College
Teaching Assistant *Sep 2021 – Dec 2022*

- Served as TA for the graduate-level seminar *Security & Privacy in Machine Learning.*
- Mentored graduate students through regular office hours, providing direct technical assistance on novel research ideation and system implementation.

Department of Computer Science and Engineering, BRAC University, Bangladesh
Lecturer *Sep 2019 – Aug 2021*

- Served as the primary instructor for *Computer Graphics* across 4 semesters, managing 4 sections and instructing approximately 400 students each semester.
- Modernized the course curriculum to reflect recent field advancements and adapted the teaching approach for pandemic-era remote learning environments.
- Redesigned the examination framework and assessment questions to fit the requirements and maintain the integrity of online evaluation systems.

Professional and Academic Service

- Program Committee, IEEE Conference on Secure and Trustworthy Machine Learning (SaTML) 2027
- Artifact Evaluation Committee, USENIX Security Symposium 2026
- Poster Committee, IEEE Security & Privacy 2026
- Assistant Program Co-ordinator, Bangladesh Mathematical Olympiad Committee (2014 - 2017)
  - Oversaw question generation for the national competition; vetted, edited, and contributed original mathematical problems.

Research Artifacts

[1] Record-Level Attribute Inference Vulnerability Estimation and Mitigation — USENIX Security 2026.
Artifact evaluated: Available, Functional, Reproduced.
https://doi.org/10.5281/zenodo.17905132

[2] Disparate Privacy Vulnerability: Targeted Attribute Inference Attacks and Defenses — USENIX Security 2025.
Artifact evaluated: Available, Functional, Reproduced.
https://doi.org/10.5281/zenodo.14732955

[3] FLShield: Validation-based defense against poisoning in federated learning.
https://github.com/ehsanul9511/FLShield

[4] CSMIA and LOMIA: Black-box model inversion attribute inference attacks.
https://github.com/smehnaz/Black-box-Model-Inversion-Attribute-Inference

Technical Skills

- **ML & AI Libraries**: Pytorch, Transformers, Scikit-Learn, JAX, XGBoost, LightGBM
- **Security & Privacy Frameworks**: Differential Privacy (Opacus), Federated Learning (Flower, TFF)
- **Programming & Scripting**: Python, C++, R, Swift, Shell
- **Data Visualization & Utility Libraries**: Pandas, Seaborn, Matplotlib, Numpy, Scipy
- **Systems & Cloud Computing**: Docker, Git, Google Cloud

Awards & Honors

2026	Future Leader, ACM AI Leadership Summit
2025, 2026	USENIX Security Symposium Travel Grant
2024	IEEE Security & Privacy Symposium Travel Grant
2012, 2013	Honorable mention in Asia Pacific Math Olympiad